Provably Authenticated Group Diffie-Hellman Key Exchange

Emmanuel Bresson (ENS)

O. Chevassut (UCL - LBNL)

D. Pointcheval (ENS)

J.-J. Quisquater (UCL)

8h ACM-CCS --- November 5-8, 2001 --- Philadelphia, USA

Passer à la première page

Outline

- Introduction
- Related work
- Model
- Security definitions
- A secure group Diffie-Hellman scheme
- Mutual authentication
- Conclusion

Introduction

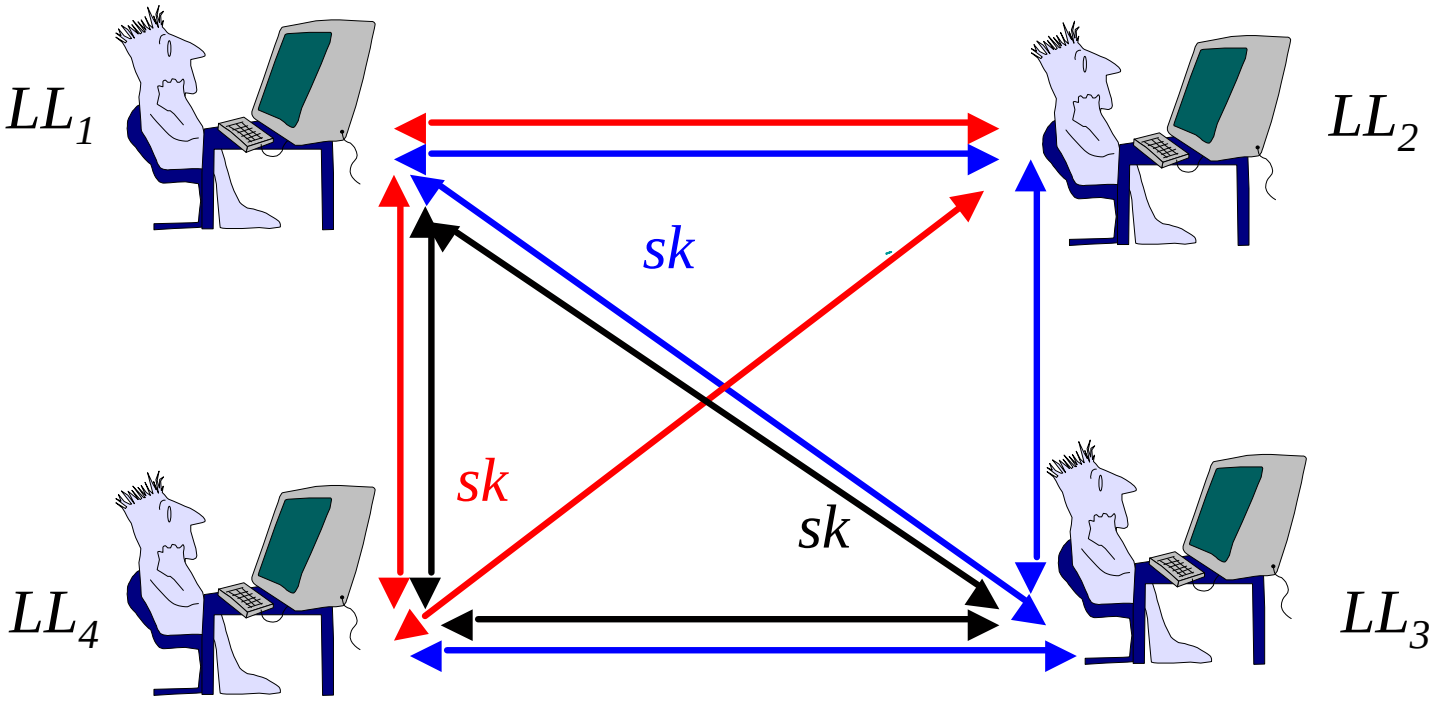
- Distributed applications need to communicate within groups
  - Collaboration and videoconferencing tools
  - Stock market, air traffic control
  - Distributed computations, GRIDS
- Increasing security requirements
  - Privacy of data
  - Protection from hackers (public network)
  - Protection against trojan horses and viruses
- Group communication must address security needs

Related Work

- Two formal models
  - Bellare-Rogaway [BR93]
  - Shoup's simulatability [Sho99]
- Group Diffie-Hellman Characteristics
  - All the members join the group at once
  - Membership is know in advance
  - Group relatively small (up to 100 members)
  - Memnbers have similar computing power
  - No hierarchy and many-to-many communication
  - No centralized server

Model of Communication

- A set of n players which have many instances
- Each player holds a long-lived key



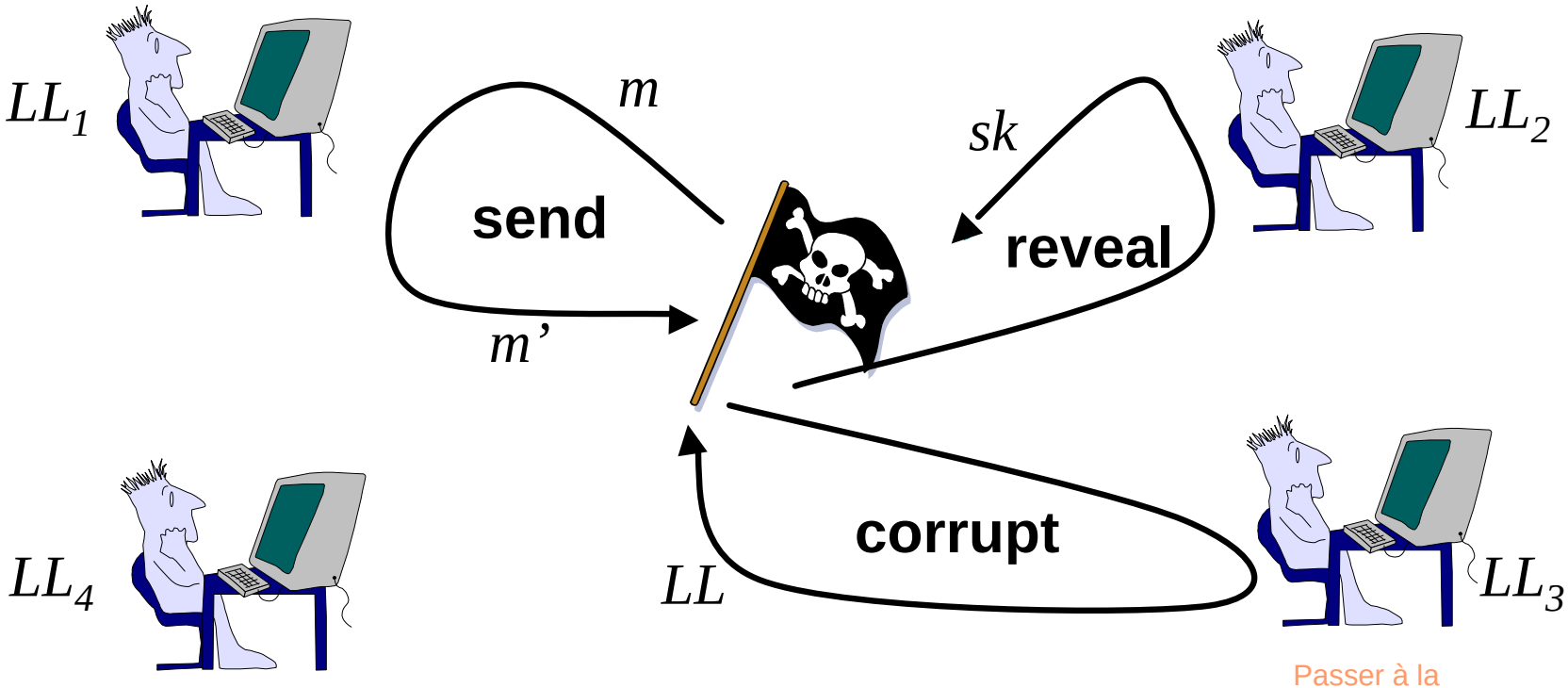
Adversarial Model

- Adversary capabilities modelled via queries

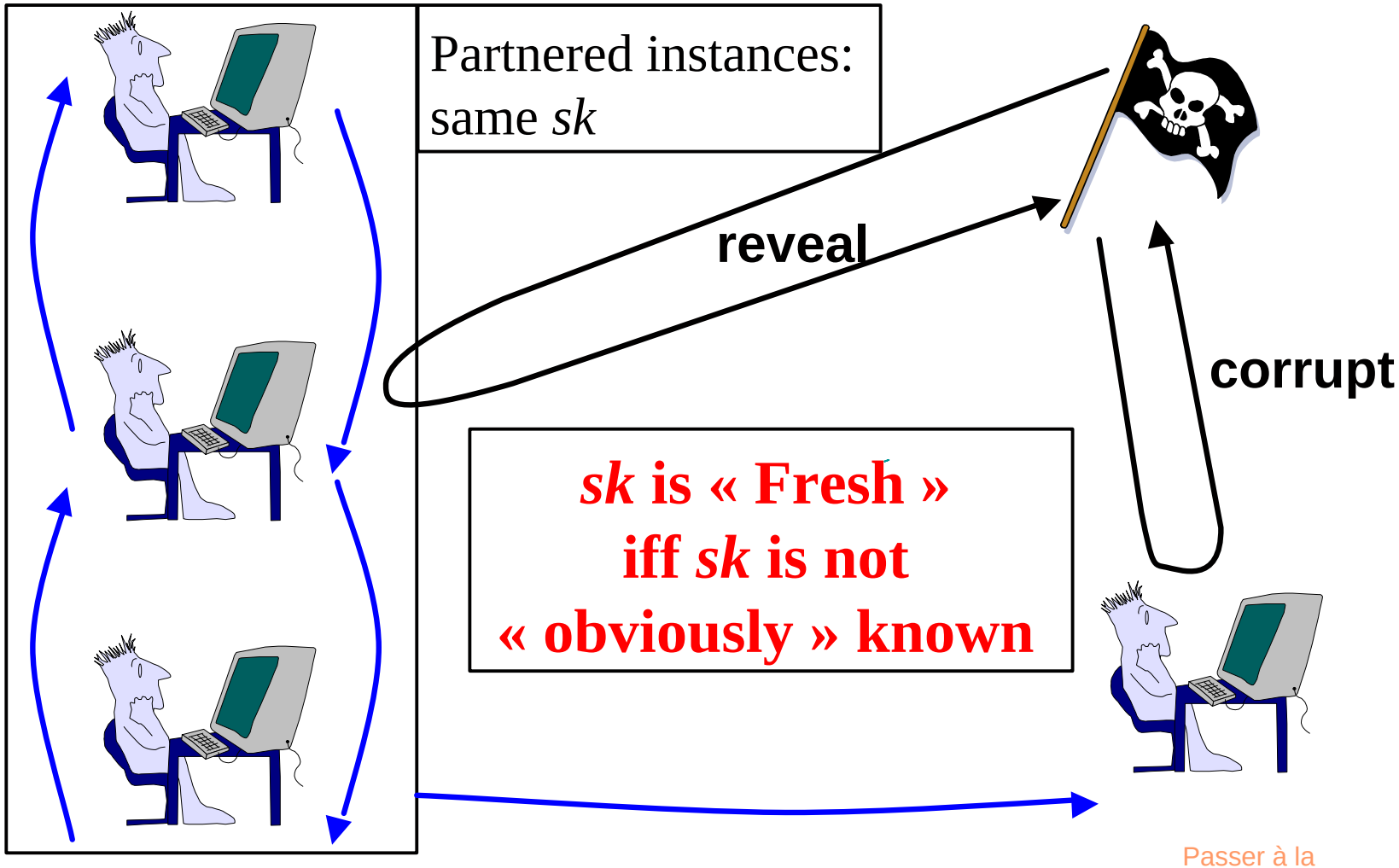
  send: send messages to instances

  reveal: obtain an instance's session key

  corrupt: obtain a player's long-lived key



Partnering / Freshness



Passer à la première page

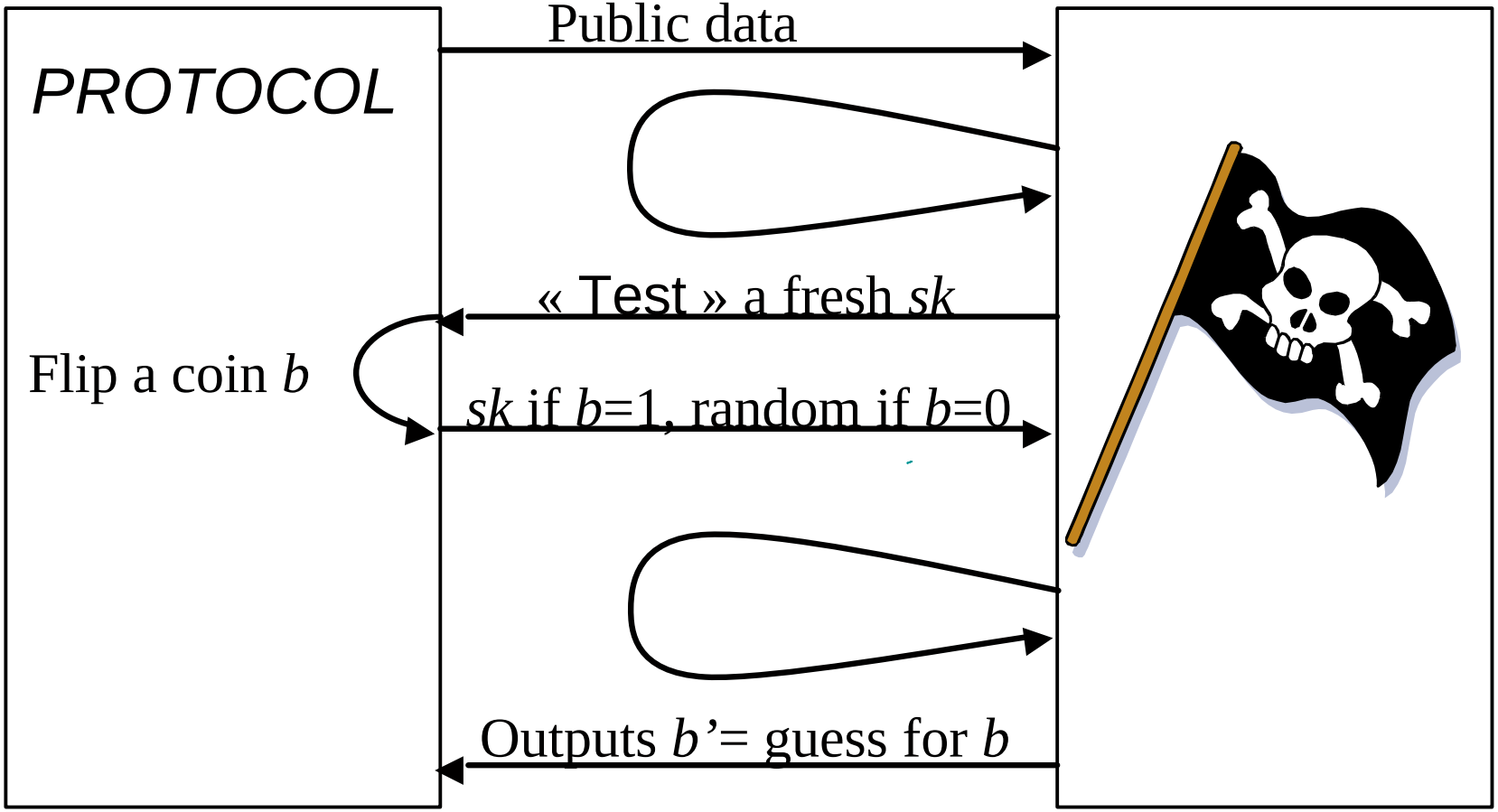
Security Definitions

- Authenticated Key Exchange (AKE)
  - Implicit Authentication:

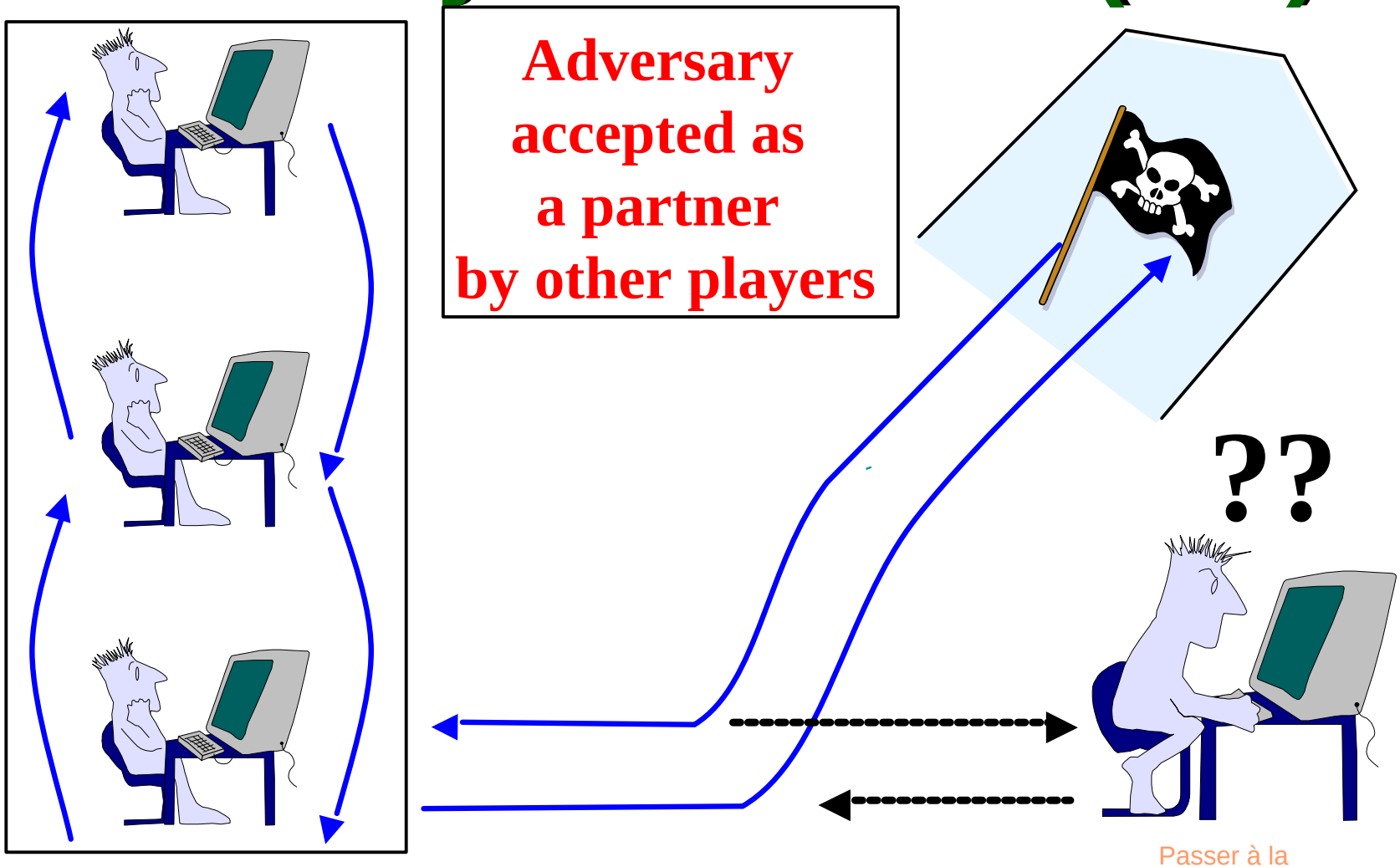
    Only the intended partners can compute sk
  - Semantic security:

    A fresh session key is undistinguishable from a random string
- Mutual Authentication (MA)
  - Each player is convinced of the identity of his partners

Security Definitions (AKE)



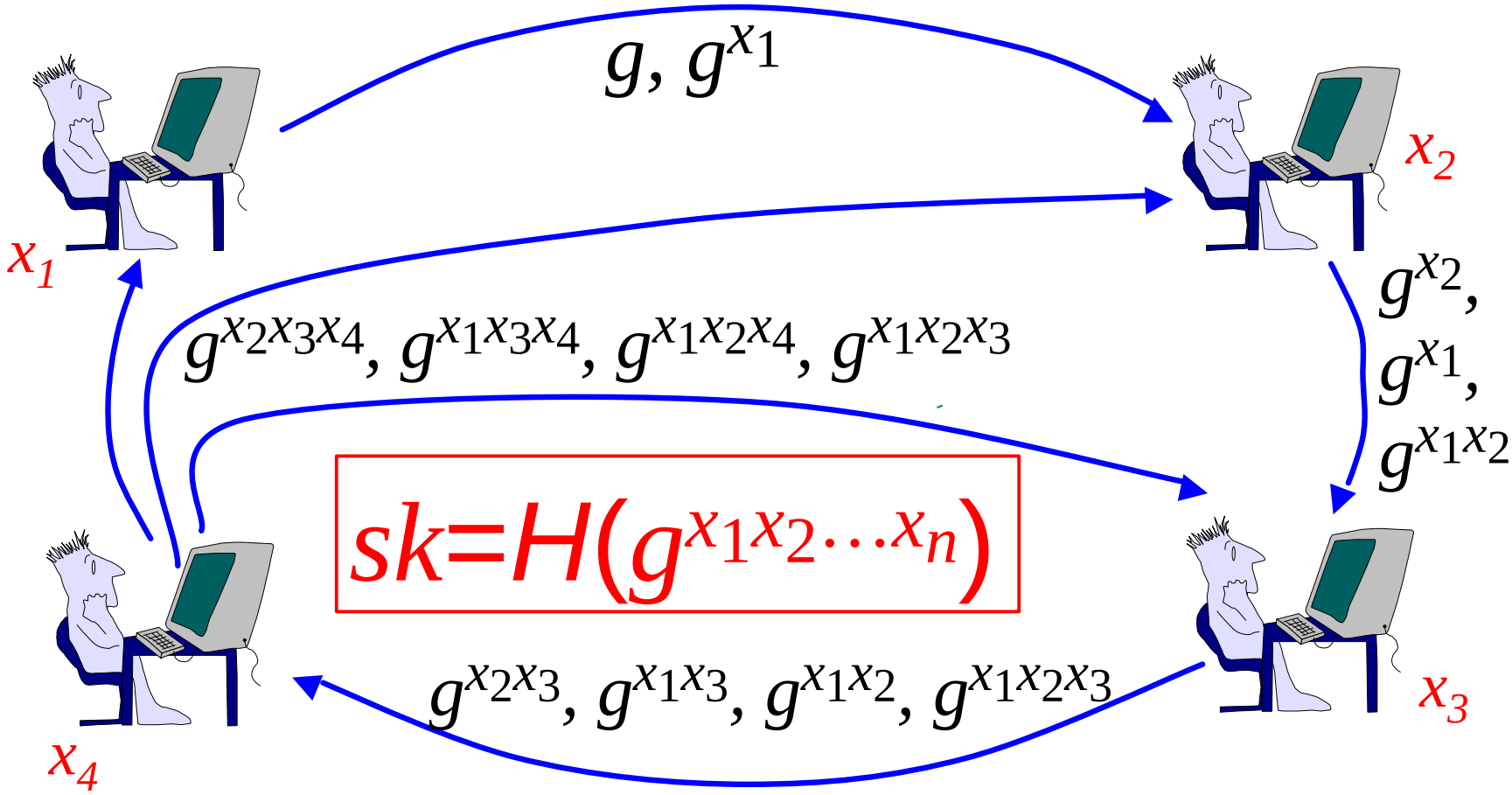
Security Definitions (MA)



A Secure Group DH Scheme

- The common session key is:
  - $sk = H(g^{x_1 x_2 \cdots x_n})$
- An algorithm (ring-based with signed flows)
  - Up-flow: U_i raises received values to the power of its x_i and forwards the result
  - Down-flow: U_n processes the last up-flow and broadcasts the result
  - Players computes the session key from values in the broadcast

A Secure Group DH Scheme



Security results (AKE)

- Proof in the Random-oracle model
  - An adversary can break AKE in two ways:
    1. Forge flows without corrupt=> forgery
    2. Guess the bit b involved in the Test-query
       => Group Diffie-Hellman problem
- Authenticated Key Exchange
  - $\mathrm{Adv}^{\mathrm{ake}}(t,q_s,q_h) \leq n \cdot \mathrm{Succ}^{\mathrm{cma}}(t') + 2 \cdot q_s^{\,n} \cdot q_h \cdot \mathrm{Succ}^{\mathrm{gcdh}}(t'')$
  - $t',t'' \leq t + q_s \cdot n \cdot T_{\exp}(k)$

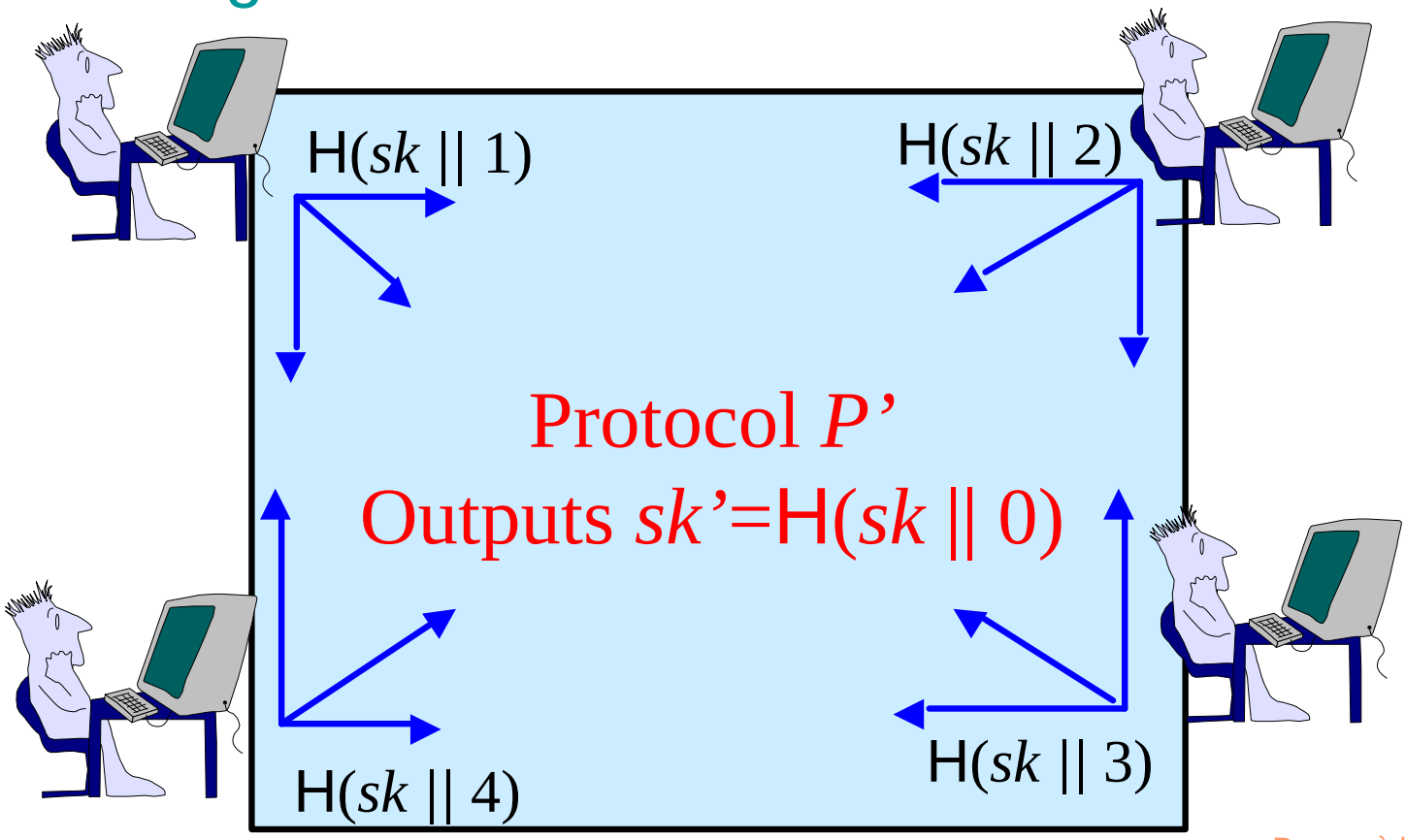
Mutual Authentication (MA)

- Insurance that other members actually computed *sk*
  - Receipt is needed => « key confirmation »
  - Receipt computed from a common secret

    => « authenticator »
- Avoid impersonate attacks
  - Only the intended partners are able to authenticate
  - Session key is computed after authentication

Mutual Authentication

- A generic transformation



Security Results (MA)

- Proof in the Random-Oracle model
  - Adversary can break MA by guessing authenticator
  - Probability at most $q_h/2^l$ per player
- Mutual authentication:
  - $\mathrm{Adv}^{\mathrm{ake}'}(t',q_s,q_h) \;?\; \mathrm{Adv}^{\mathrm{ake}}(t,q_s,q_h) + q_h\cdot/2^l$
  - $\mathrm{Succ}^{\mathrm{ma}}(t',q_s,q_h) \;?\; \mathrm{Adv}^{\mathrm{ake}}(t,q_s,q_h) + n\cdot q_h\cdot/2^l$
  - $t',t'' \;?\; t + (q_s + q_s)\cdot O(1)$

Conclusion

- Limitations : static case
  - Random oracle model
  - Efficiency: does not handle incremental membership changes
- More general scenario
  - Members join and leave at any time
  - E. Bresson, O. Chevassut and D. Pointcheval, *Provably Authenticated Group Diffie-Hellman Key Exchange – The Dynamic Case*, to appear at Asiacrypt ’01, Dec 9—13, 2001